FORTINET
High Performance Network Security

FortiOS™ Handbook - FortiView

VERSION 5.4.1

FORTIOS
5.4
VERSION

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Friday, June 17, 2016

FortiOS™ Handbook - FortiView

01-540-122872-20160616

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-09-01	Official release for FortiOS 5.4.
2016-06-14	Official release for FortiOS 5.4.1.

Introduction

This document provides a general guide to FortiView, the FortiOS log view tool, explaining its layout, features, and its usefulness in everyday administrative scenarios. This document includes:

- Overview on page 18 outlines the role FortiView plays in FortiOS and its overall layout. This section also identifies which FortiGate platforms support the full FortiView features.
- FortiView consoles on page 29 describes the various FortiView consoles available in FortiOS, including example scenarios, in most cases.
- Reference on page 44 explains reference information for the various consoles in FortiView, and describes the assortment of filtering options, drilldown options, and columns available.
- Troubleshooting FortiView on page 55 offers solutions to common technical issues experienced by FortiGate users regarding FortiView.

What's new in FortiOS 5.4

New Consoles

In FortiOS 5.4, a variety of new consoles have been added to FortiView:

FortiView Policies console

The new **Policies** console works similarly to other FortiView consoles, yet allows administrators to monitor policy activity, and thereby decide which policies are most and least active. This helps the administer to discern which policies are unused and can be deleted.

In addition, you have the ability to click on any policy in the table to drill down to the Policies list and view or edit that policy. You can view this new console in either Table or Bubble Chart view.

FortiView Interfaces console

The new **Interfaces** console works similarly to other FortiView consoles and allows administrators to perform current and historical monitoring per interface, with the ability to monitor bandwidth in particular. You can view this new console in either Table or Bubble Chart view.

FortiView Countries console

A new **Countries** console has been introduced to allow administrators to filter traffic according to source and destination countries. This console includes the option to view the Country Map visualization (see below).

FortiView Device Topology console

The new **Device Topology** console provides an overview of your network structure in the form of a Network Segmentation Tree diagram (see below).

FortiView Traffic Shaping console

A new **Traffic Shaping** console has been introduced to improve monitoring of existing Traffic Shapers.

Information displayed includes Shaper info, Sessions, Bandwidth, Dropped Bytes, and more.

FortiView Threat Map console

A new **Threat Map** console has been introduced to monitor risks coming from various international locations arriving at a specific location, depicted by the location of a FortiGate on the map (see below).

FortiView Failed Authentication console

A **Failed Authentication** console has been added under **FortiView** that allows you to drill down an entry to view the logs. This new console is particularly useful in determining whether or not the FortiGate is under a brute force attack. If an administrator sees multiple failed login attempts from the same IP, they could (for example) add a local-in policy to block that IP.

The console provides a list of unauthorized connection events in the log, including the following:

- unauthorized access to an admin interface (telnet, ssh, http, https, etc.)
- failure to query for SNMP (v3) or outside of authorized range (v1, v2, v3)
- failed attempts to establish any of the following:
  - Dial-up IPsec VPN connections
  - Site-to-site IPsec VPN connections
  - SSL VPN connections
  - FGFM tunnel

FortiView WiFi Clients console

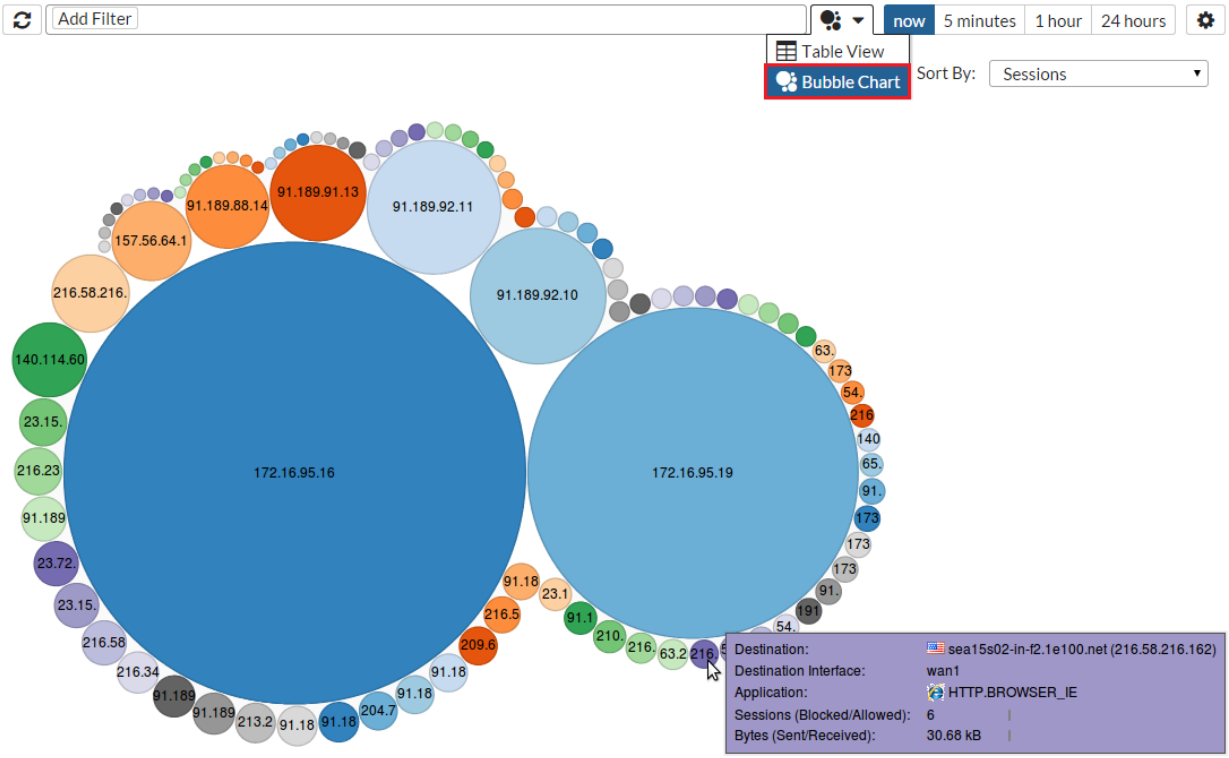
The WiFi Clients console has been added to FortiView in FortiOS 5.4. As you might expect, you can use this console to display top wireless user network usage and information. You can drilldown to filter the information that is displayed.

Information displayed includes Device, Source IP, Source SSID, AP, and more.

New FortiView Visualizations

New visualization support has been added to FortiView via the Bubble Chart and the Country Map.

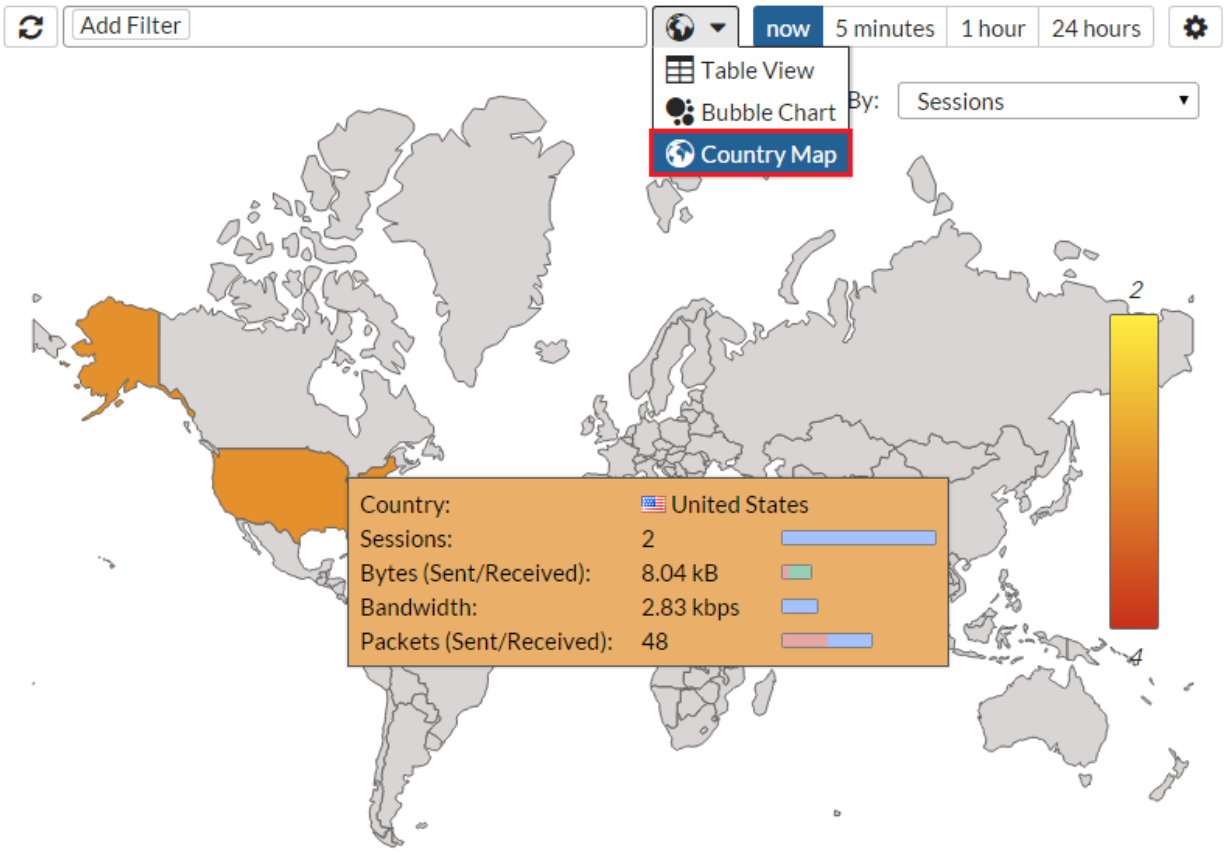
Bubble Chart Visualization



Notes about the Bubble Chart:

- It is possible to sort on the Bubble Chart using the **Sort By:** dropdown menu.
- The size of each bubble represents the related amount of data.
- Place your cursor over a bubble to display a tool-tip with detailed info on that item.
- You can click on a bubble to drilldown into greater (filtered) detail.

Country Map Visualization



Notes about the Country Map:

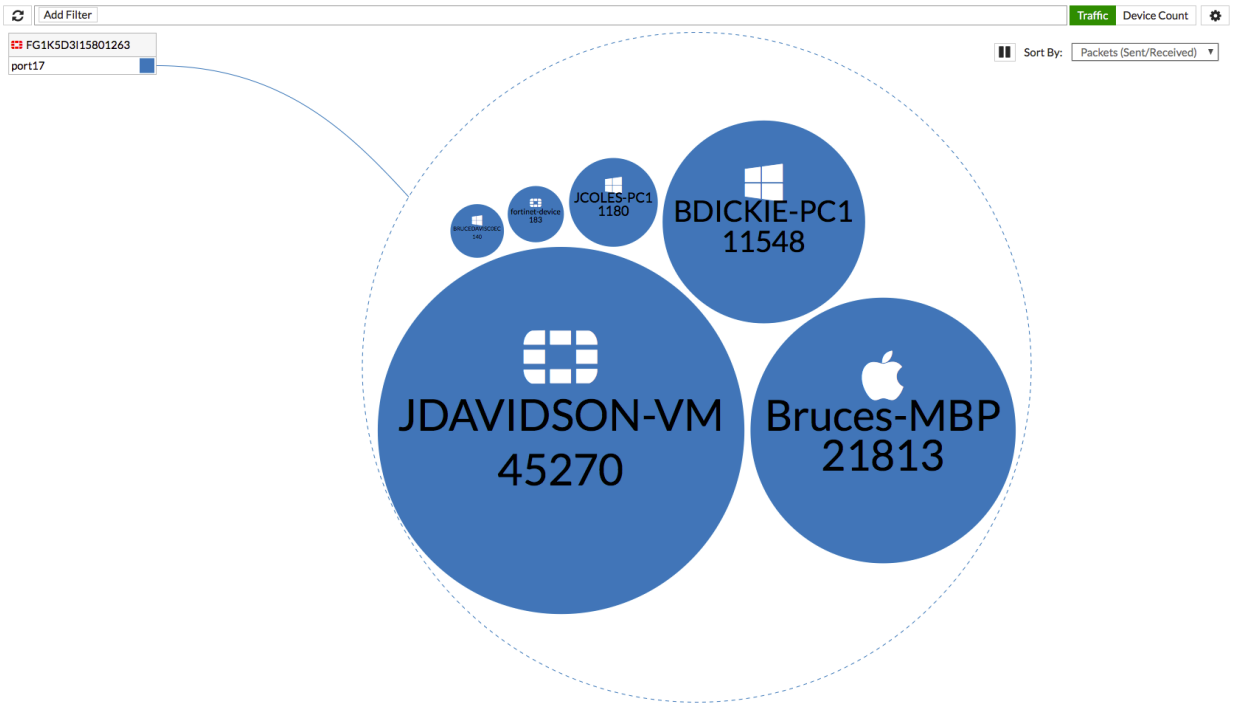
- The Country Map is only available in the Countries dashboard.
- It is possible to sort on the Country Map using the **Sort By:** dropdown menu.
- Place your cursor over any country to display a tool-tip with detailed info on that country's traffic.
- The colour gradiant on the map indicates the traffic load, where red indicates the more critical load.
- Click on any country to drilldown into greater (filtered) detail.

Threat Map Visualization

Notes about the Threat Map:

- Threats from various international destinations will be shown, but only those arriving at your destination, as depicted by the FortiGate.
- Place your cursor over the FortiGate's location to display the device name, the IP address, and the city name/location.
- A visual lists of threats is shown at the bottom, displaying the location, severity, and nature of the attacks.
- The colour gradiant of the darts on the map indicate the traffic risk, where red indicates the more critical risk.
- Click on any country to drilldown into greater (filtered) detail.

Device Topology Visualization



Notes about Device Topology:

- Place your cursor over any object in the visualization to display the device name, the IP address, Sessions, sent and received Bytes and Packets, Bandwidth, and Dropped Bytes.
- In many cases, such as Internal Network Firewall (INFW) deployments, there are multiple Fortigates performing NAT before a host reaches the external-facing WAN. In such a situation, a bubble chart depicting internal traffic may be inaccurate because the biggest bubble will be a Fortigate that is NAT'ing hundreds of endpoints behind it. This page solves that issue by ensuring all network elements are given visibility and structured in a human-readable format.

Realtime visualization

In addition to these new visualization options, you can now also enable realtime visualization.

To enable realtime visualization:

1. Click on the **Settings** icon next to the upper right-hand corner and select **Auto update realtime visualizations**. An option is displayed to set the **Interval (seconds)**. The maximum value is 300.
2. Enter a desired **Interval** and click **Apply**.

Links created between FortiView and View/Create Policy

The **Policy** column in FortiView consoles and the Log Viewer pages has changed to a link, which navigates to the IPv4 or IPv6 policy list and highlights the policy.

Right-clicking on a row in FortiView or the Log Viewer has menu items for **Block Source**, **Block Destination** and **Quarantine Source** where appropriate columns are available to determine these values. When multiple rows are selected, the user will be prompted to create a named **Address Group** to contain the new addresses.

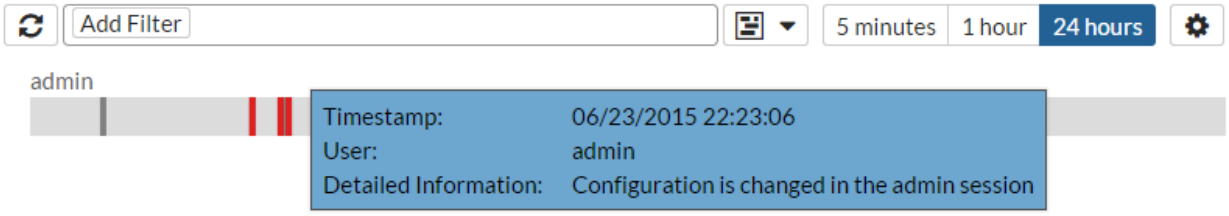
When the user clicks **Block Source** or **Block Destination** they are taken to a policy creation page with enough information filled in to create a policy blocking the requested IP traffic.

The policy page will feature an informational message block at the top describing the actions that will be taken. Once the user submits the form, the requisite addresses, groups and policy will be created at once.

If the user clicks on **Quarantine User** then they will be prompted for a duration. They may also check a box for a **Permanent Ban**. The user can manage quarantined users under **Monitor > User Quarantine Monitor**.

Visualization support for the Admin Logins page

A useful chart is now generated for Admin login events under **FortiView > Admin Logins**. You can view the information in either **Table View** or **Timeline View** (shown below). In Timeline View, each line represents on administrator, with individual sessions indicated per administrator line. When you hover over a particular timeline, detailed information appears in a tooltip.



New bandwidth column added to realtime FortiView pages

The FortiView console provides a new bandwidth column that displays information for bandwidth calculated on a per-session level, providing administrators the ability to sort realtime bandwidth usage in descending order.

Accelerated session filtering on All Sessions page

By default, on a FortiGate unit with NP6 processors, when you enable traffic logging in a firewall policy this also enables NP6 per-session accounting. If you disable traffic logging this also disables NP6 per-session accounting. This behavior can be changed using the following command:

```
config system np6
   edit np6_0
      set per-session-accounting {disable | all-enable | enable-by-log}
   end
```

By default, `per-session-accounting` is set to `enable-by-log`, which results in per-session accounting being turned on when you enable traffic logging in a policy. This configuration is set separately for each NP6 processor.

When offloaded sessions appear on the FortiView All Sessions console they include an icon identifying them as NP sessions:

Application	Bytes (Sent/Received)	Policy
TCP/443	29.16 kB	Local In
YouTube	NP 219.44 kB	my-policy
UDP/53	31.05 kB	Local In

You can hover over the NP icon to see some information about the offloaded sessions.

You can also use a FortiASIC Filter to view just the accelerated sessions.

WHOIS Lookup anchor for public IPv4 addresses

Reverse IP lookup is now possible in FortiOS 5.4. A WHOIS lookup icon is available when you mouse over a public IP address in a FortiView log. If you left-click on the lookup icon, a new tab is opened in your browser for www.networksolutions.com, and a lookup is performed on the selected IP address (this option persists after drilling down one level in FortiView).

FortiGuard Cloud App DB identification

FortiView now recognizes FortiGuard Cloud Application database traffic, which is mainly monitored and validated by FortiFlow, an internal application that identifies cloud applications based on IP, Port, and Protocol. Administrators can potentially use this information for WAN Link Load Balancing, for example.

7-day time display

In FortiOS 5.4, the following FortiGate models now support 7-day time display:

- FortiGate 1000D
- FortiGate 1500D
- FortiGate 3700DX
- FortiGate 3700D

The option for 7-day time display, however, can only be configured in the CLI using the following command:

```
config log setting
   set fortiview-weekly-data {enable|disable}
end
```

NP4 and NP6 icons showing accelerated sessions (282180)

When viewing sessions in the All Sessions console, information pertaining to NP4/ NP6 acceleration is now reflected via an appropriate icon. The tooltip for the icon includes the NP chip type and its total number of accelerated sessions.

Filtering on accelerated sessions (282180)

In addition to NP4/NP6 icons, you can now filter the console on 'FortiASIC' ('Accelerated' versus 'Not Accelerated') sessions.

WHOIS Lookup anchor for public IPv4 addresses (282701)

Reverse IP lookup is now possible in FortiOS 5.4. A WHOIS lookup icon is available when you mouse over a public IP address in a FortiView log. If you left-click on the lookup icon, a new tab is opened in your browser for www.networksolutions.com, and a lookup is performed on the selected IP address (this option persists after drilling down one level in FortiView).

New Report database construction (280398 267019)

This will improve performance with reports and FortiView without requiring any configuration changes.

Added a Timeline graph for admin events (271389)

Improved monitoring of traffic shapers; added traffic shaping to FortiView (290363)

Failed Authentication Attempts are now visible in FortiView (265890)

Added bandwidth column to FortiView (260896)

FortiView now displays Quarantine Source and appropriate icon in lists (289206)

Purpose

FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view on your FortiGate. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

FortiView allows you to use multiple filters within the consoles, enabling you to narrow your view to a specific time (up to 24 hours in the past), by user ID or local IP address, by application, and many more. For more on FortiView's filtering options, see Filtering options on page 44

FortiView can be used to investigate traffic activity, such as user uploads/downloads or videos watched on YouTube, on a network-wide, user group, and individual-user level, with information relayed in both text and visual format. FortiView makes it easy to get an actionable picture of your network's internet activity.

The degree to which information can be logged will depend on which FortiGate unit you have. For more information, see Enabling FortiView on page 18.

Overview

This section provides an overview of FortiView, its interface, and options, including the following:

Enabling FortiView

By default, FortiView is enabled on FortiGates running FortiOS firmware version 5.2 and above. You will find the FortiView consoles in the main menu. However, certain options will not appear unless the FortiGate has **Disk Logging** enabled.

Only certain FortiGate models support Disk Logging. A complete list of FortiGate platforms that support Disk Logging is provided in the matrix below.

To enable Disk Logging

1. Go to **Log & Report > Log Settings** and select the checkbox next to **Disk**.
2. **Apply** the change.

To enable Disk Logging - CLI

```
config log disk setting
   set status enable
end
```

FortiView Feature Support - Platform Matrix

Note that the following table identifies three separate aspects of FortiView in FortiOS 5.2.3:

- Basic feature support
- Historical Data
- Disk Logging

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG/FWF-20C Series	✔		
FG/FWF-30D/40C Series	✔		
FG/FWF-60C Series	✔		

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG/FWF-60D Series	✔		
FGR-60D	✔		
FG-60D	✔		
FG/FWF-80C Series	✔		
FG-80D	✔	✔	1 hour
FG/FWF-90D Series	✔	✔	1 hour
FG/FWF-92D Series	✔		
FG-110C	✔		
FG-111C	✔	**CLI**	1 hour
FG-100D Series	✔	✔	24 hours
FG-200B Series	✔	**#**	**#** (24 hours)
FG-200D Series	✔	✔	24 hours
FG-310B	✔		**#** (24 hours)
FG-311B	✔		**#** (24 hours)
FG-300C	✔	✔	24 hours
FG-300D	✔	✔	24 hours
FG-500D	✔	✔	24 hours
FG-620B	✔	**#**	**#** (24 hours)
FG-621B	✔	**#**	**#** (24 hours)
FG-600C	✔	✔	24 hours
FG-800C	✔	✔	24 hours
FG-1000D	✔	✔	7 hours, 24 hours
FG-1500D	✔	✔	7 hours, 24 hours
FG-1240B	✔	✔	24 hours

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG-3016B	✔	**#**	**#** (24 hours)
FG-3040B	✔	**CLI**	24 hours
FG-3140B	✔	**CLI**	24 hours
FG-3240C	✔	**CLI**	24 hours
FG-3600C	✔	**CLI**	24 hours
FG-3700D/DX	✔	**CLI**	7 hours, 24 hours
FG-3810A	✔	**#**	**#** (24 hours)
FG-3950B	✔	**#, CLI**	**#** (24 hours)
FG-3951B	✔	**#, CLI**	**#** (24 hours)
FG-5001A	✔	**#, CLI**	**#** (24 hours)
FG-5001B	✔	**CLI**	24 hours
FG-5001C	✔	**CLI**	24 hours
FG-5001D	✔	**CLI**	24 hours
FG-5101C	✔	**CLI**	24 hours
FS-5203B	✔	**CLI**	

✔ = *Default support.*
= *Local storage required.*

* Refer to section on Historical Data below.

Basic feature support

FortiView's consoles give insight into your user's traffic, not merely showing which users are creating the most traffic, but what sort of traffic it is, when the traffic occurs, and what kind of threat the traffic may pose to the network.

FortiView basic feature support consists of the following consoles:

- Sources
- Destinations
- Interfaces
- Policies
- Countries

- All Sessions
- Applications

The complete array of features in FortiView requires disk logging enabled (see below). It includes those consoles listed above as well as the following:

- WiFi Clients
- Cloud Applications
- Web Sites
- Threats
- Failed Authentication
- System Events
- Admin Logins
- VPN

Historical Data

Not all consoles have the same available historical data options, depending on whether or not your traffic is locally stored.

Below is a table showing which features are available for units using local storage, including the historical data options.

Only FortiGate models 100D and above support the 24 hour historical data.

Features	With Local Storage				Without Local Storage			
	Now	5 min	1 hr	24 hr *	Now	5 min	1 hr	24 hr
Sources	✔	✔	✔	✔	✔			
Destinations	✔	✔	✔	✔	✔			
Interfaces	✔	✔	✔	✔				
Policies	✔	✔	✔	✔				
Countries	✔	✔	✔	✔				
All Sessions	✔	✔	✔	✔	✔			
Applications	✔	✔	✔	✔	✔			
WiFi Clients		✔	✔	✔				
Cloud Applications	✔	✔	✔	✔	✔			

Features	With Local Storage				Without Local Storage			
	Now	5 min	1 hr	24 hr *	Now	5 min	1 hr	24 hr
Web Sites	✔	✔	✔	✔				
Threats		✔	✔	✔				
Threat Map	✔				✔			
FortiSandbox		✔	✔	✔				
Failed Authentication		✔	✔	✔				
System Events		✔	✔	✔				
Admin Logins		✔	✔	✔				
VPN		✔	✔	✔				

* Not available for desktop models with SSD.

7-day time display

As mentioned previously, certain models support 7-day time display. These models are listed below:

- FortiGate 1000D
- FortiGate 1500D
- FortiGate 3700DX
- FortiGate 3700D

The option for 7-day time display, however, can only be configured in the CLI using the following command:

```
config log setting
   set fortiview-weekly-data {enable|disable}
end
```

Disk Logging

Only certain FortiGate models support Disk Logging (see above).

To enable Disk Logging, go to **Log & Report > Log Settings**, and select the checkbox next to **Disk** and apply the change.

Configuration Dependencies

Most FortiView consoles require the user to enable several features to produce data. The following table summarizes the dependencies:

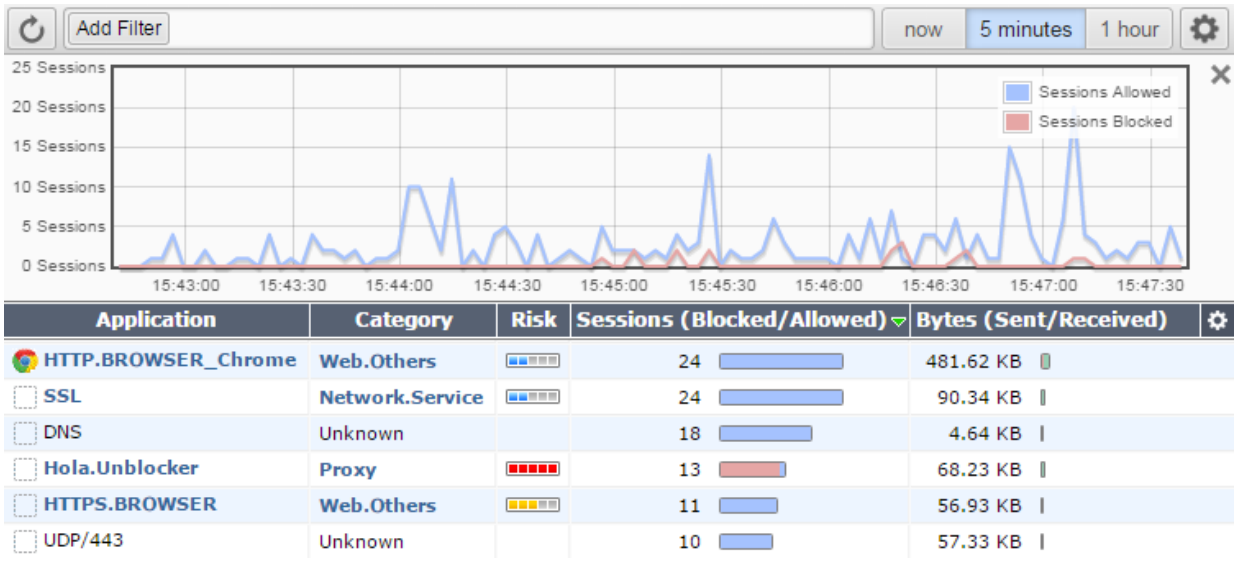
Feature	Dependencies (Realtime)	Dependencies (Historical)
Sources	None, always supported	Traffic logging enabled in policy
Destinations	None, always supported	Traffic logging enabled in policy
Interfaces	None, always supported	Disk logging enabled Traffic logging enabled in policy
Policies	None, always supported	Disk logging enabled Traffic logging enabled in policy
Countries	None, always supported	Disk logging enabled Traffic logging enabled in policy
All Sessions	None, always supported	Traffic logging enabled in policy
Applications	None, always supported	Disk logging enabled Traffic logging enabled in policy Application control enabled in policy
WiFi Clients	None, always supported	Disk logging enabled Traffic logging enabled in policy
Cloud Applications	Not supported	Disk logging enabled Application control enabled in policy SSL "deep inspection" enabled in policy Deep application inspection enabled in application sensor Extended UTM log enabled in application sensor
Web Sites	Disk logging enabled Web Filter enabled in policy "web-url-log" option enabled in Web Filter profile	Disk logging enabled Web Filter enabled in policy "web-url-log" option enabled in Web Filter profile

Feature	Dependencies (Realtime)	Dependencies (Historical)
Threats	Not supported	Disk logging enabled Traffic logging enabled in policy Threat weight detection enabled
Threat Map	None, always supported	Disk logging enabled Traffic logging enabled in policy Threat weight detection enabled
FortiSandbox	Not supported	Disk logging enabled Traffic logging enabled in policy
Failed Authentication	Not supported	Disk logging enabled
System Events	Not supported	Disk logging enabled
Admin Logins	Not supported	Disk logging enabled
VPN	Not supported	Disk logging enabled Traffic logging enabled in policy

FortiView interface

FortiView lets you access information about the traffic activity on your FortiGate, visually and textually. FortiView is broken up into several consoles, each of which features a top menu bar and a graph window, as seen in the following image:

FortiView Application console sorted by Sessions (Blocked/Allowed)



The top menu bar features:

- a **Refresh** button, which updates the data displayed,
- a **Filter** button, for filtering the data by category,
- a **Settings** button (containing additional viewing settings and a link to the Threat Weight menu).
- a drop-down menu of different views:
  - **Time Display** (options: now, 5 minutes, 1 hour, or 24 hours),
  - **Table View**
  - **Timeline View**
  - **Bubble Chart**[1]
  - **Country Map**[2]

[1] For information on the Bubble Chart, refer to Bubble Chart Visualization on page 26.

[2] For more information on the Country Map, refer to Countries on page 33.

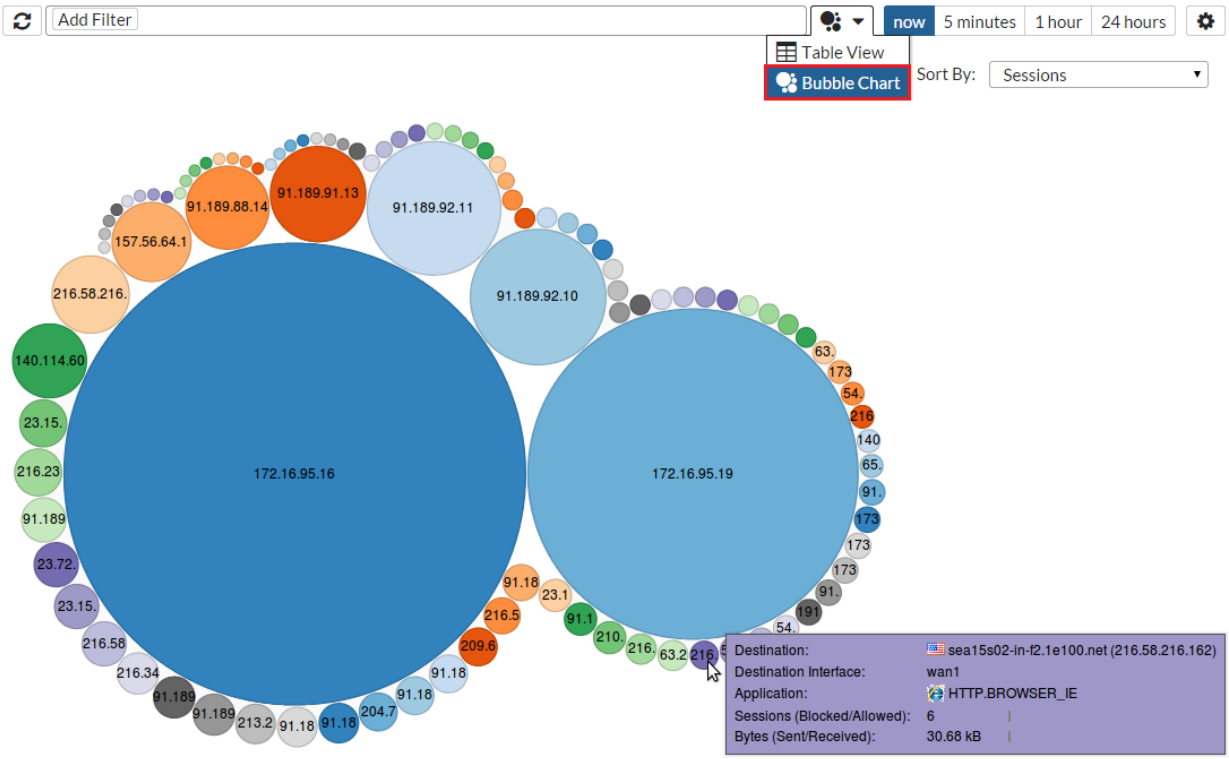
Certain views are only available in specific consoles.

The FortiView graph

The graph window can be hidden using the **X** in the top right corner, and re-added by selecting **Show Graph**. To zoom in on a particular section of the graph, click and drag from one end of the desired section to the other. This will appear in the **Time Display** options as a **Custom** selection. The minimum selection size is 60 seconds.

Only FortiGate models 100D and above support the 24 hour historical data.

Bubble Chart Visualization



Notes about the Bubble Chart:

- It is possible to sort on the Bubble Chart using the **Sort By:** dropdown menu.
- The size of each bubble represents the related amount of data.
- Place your cursor over a bubble to display a tool-tip with detailed info on that item.
- You can click on a bubble to drilldown into greater (filtered) detail.

Links created between FortiView and View/Create Policy

The **Policy** column in FortiView consoles and the Log Viewer pages includes a link, which navigates to the IPv4 or IPv6 policy list and highlights the policy.

Right-clicking on a row in FortiView or the Log Viewer has menu items for **Block Source**, **Block Destination** and **Quarantine Source** where appropriate columns are available to determine these values. When multiple rows are selected, the user will be prompted to create a named **Address Group** to contain the new addresses.

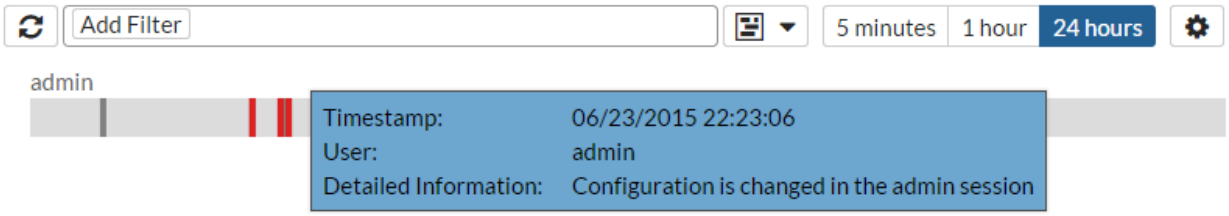
When the user clicks **Block Source** or **Block Destination** they are taken to a policy creation page with enough information filled in to create a policy blocking the requested IP traffic.

The policy page will feature an informational message block at the top describing the actions that will be taken. Once the user submits the form, the requisite addresses, groups and policy will be created at once.

If the user clicks on **Quarantine User** then they will be prompted for a duration. They may also check a box for a **Permanent Ban**. The user can manage quarantined users under **Monitor > User Quarantine Monitor**.

Visualization support for the Admin Logins page

A useful chart is generated for Admin login events under **FortiView > Admin Logins**. You can view the information in either **Table View** or **Timeline View** (shown below). In Timeline View, each line represents on administrator, with individual sessions indicated per administrator line. When you hover over a particular timeline, detailed information appears in a tooltip.



Realtime visualization

To enable realtime visualization:

1. Click on the **Settings** icon next to the upper right-hand corner and select **Auto update realtime visualizations**. An option is displayed to set the **Interval (seconds)**. The maximum value is 300.
2. Enter a desired **Interval** and click **Apply**.

Accelerated sessions

When viewing sessions in the All Sessions console, information pertaining to NP4/ NP6 acceleration is now reflected via an appropriate icon in the table. The tooltip for the icon includes the NP chip type and its total number of accelerated sessions.

Filtering on accelerated sessions

You can filter the console on 'FortiASIC' ('Accelerated' versus 'Not Accelerated') sessions.

WHOIS Lookup anchor for public IPv4 addresses

A Reverse IP lookup is possible using the WHOIS lookup icon available when you mouse over a public IP address in a FortiView log. If you left-click on the lookup icon, a new tab is opened in your browser for www.networksolutions.com, and a lookup is performed on the selected IP address (this option persists after drilling down one level in FortiView).

FortiView consoles

This section describes the following log filter consoles available in FortiView:

- "Physical Topology" on page 30 graphically displays the physical structure of your network by device, as part of the Co-operative Security Fabric feature set.
- "Logical Topology" on page 30 graphically displays the logical structure of your network by connection, as part of the Co-operative Security Fabric feature set.
- Sources on page 31 displays detailed information on the sources of traffic passing through the FortiGate, and the section covers how you can investigate an unusual spike in traffic to determine which user is responsible.
- Destinations on page 32 displays detailed information on user destination-accessing through the use of drill down functionality.
- Interfaces on page 32 displays the number of interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring.
- Policies on page 33 displays what policies are in affect on your network, what their source and destination interfaces are, how many sessions are in each policy, and what sort of traffic is occurring.
- Countries on page 33 graphically displays network activity by geographic region.
- WiFi Clients on page 35 displays a list of all the devices connected to the WLAN.
- "Traffic Shaping" on page 35 displays a list of existing Traffic Shapers, detailing their bandwidth use and which traffic is being shaped by each shaper.
- All Sessions on page 35 displays complete information on all FortiGate sessions, with the ability to filter sessions by port number and application type.
- Applications on page 36 displays Applications used on the network that have been recognized by Application Control, and this section shows how you can view what sort of applications individual employees are using.
- Cloud Applications on page 37 displays Web/Cloud Applications used on the network, and this section shows how you can drill down to access detailed data on cloud application usage, e.g. YouTube.
- Web Sites on page 38 displays websites visited as part of network traffic that have been recognized by Web Filtering, and this section shows how you can investigate instances of proxy avoidance, which is the act of circumventing blocks using proxies.
- Threats on page 38 monitors threats to the network, both in terms of their Threat Score and Threat Level.
- Threat Map on page 39 provides a geographical display of threats, in realtime, from international sources as they arrive at your FortiGate.
- Failed Authentication on page 41 displays instances in which users attempted to connect to the server but were unsuccessful.
- System Events on page 41 displays security events detected by FortiOS, providing a name and description for the events, an assessment of the event's severity level, and the number of instances the events were detected.
- Admin Logins on page 42 displays information on administrator interactions with the network, including the number of login instances, number of failed logins, and the length of time logged in.
- VPN on page 42 displays how users can access information on any VPNs associated with their FortiGate.

Physical Topology

The **Physical Topology** console displays your network as a bubble chart of interconnected devices, grouping objects based on which upstream device they are connected to, with comparative bubble size used to illustrate traffic volume. This console can be filtered by **Device Traffic**, **Device Count**, **Device Type**, or **No Devices**, which displays only networking devices.

You can mouse over a device's bubble to see its **Name**, **IP Address**, and traffic volume data. You can also double-click on any bubble to zoom it to a reasonable size, as some may be much smaller or larger based on their traffic volume.

You can sort the bubbles by **Bytes Sent/Recieved**, **Packets Sent/Received**, **Bandwidth**, **Dropped Bytes**, and **Sessions**. Some options are not available in longer historical data periods.

FortiGates and other networking devices are depicted as boxes. You can mouse over a FortiGate's box to see its **Serial Number**, **Hostname**, and **Firmware Version/Build**.

Information about upstream devices will not be available unless you properly configure the Upstream FortiGate settings in **System > Cooperative Security Fabric**.

Scenario: Determining which device is overusing bandwidth

From the **Physical Topology** console, you can use filters and sorts to narrow down the session data to look for specific information. In this example, the filters will be used to locate a device that is using excessive bandwidth.

1. Go to **FortiView > Physical Topology**.
2. Select **24 hours** from the **Time Display** options.
3. Select **Device Traffic** from the dropdown list to the left of the **Time Display** options, then sort by **Bytes (Sent/Received)**. Mouse over the largest bubble in the chart to see details about the device that has transmitted the most data.

Only FortiGate models 100D and above support the 24 hour historical data.

Logical Topology

The **Logical Topology** console displays your network as a bubble chart of network connection points, grouping objects based on which upstream device interface they are connected to, with comparative bubble size used to illustrate traffic volume. This console can be filtered by **Device Traffic**, **Device Count**, **Device Type**, or **No Devices**, which displays only networking devices.

You can mouse over a device's bubble to see its **Name**, **IP Address**, and traffic volume data. You can also double-click on any bubble to zoom it to a reasonable size, as some may be much smaller or larger based on their traffic volume.

You can sort the bubbles by **Bytes Sent/Recieved**, **Packets Sent/Received**, **Bandwidth**, **Dropped Bytes**, and **Sessions**. Some options are not available in longer historical data periods.

FortiGates and other networking devices are depicted as boxes. You can mouse over a FortiGate's box to see its **Serial Number**, **Hostname**, and **Firmware Version/Build**. Also appearing in the FortiGate box is each interface that has devices connected to it, upstream or downstream. You can mouse over the name of an interface to see its **IP Address**, **Network** (subnet), and **Role**.

Information about upstream devices will not be available unless you properly configure the Upstream FortiGate settings in **System > Cooperative Security Fabric**.

Scenario: Determining which interface is blocking sessions incorrectly

From the **Logical Topology** console, you can use filters and sorts to narrow down the session data to look for specific information. In this example, the filters will be used to locate an interface that is blocking sessions incorrectly.

1. Go to **FortiView > Logical Topology**.
2. Select **1 hour** from the **Time Display** options.
3. Select **Device Traffic** from the dropdown list to the left of the **Time Display** options, then sort by **Sessions (Blocked/Allowed)**.
4. Mouse over each bubble in the chart to see details, looking at the bar next to **Sessions (Blocked/Allowed)**. The blue portion of the bar represents Allowed sessions, and red represents Blocked. Devices connected to the interface that is blocking sessions will have a much larger red area than devices connected to other interfaces.

Only FortiGate models 100D and above support the 24 hour historical data.

Sources

The **Sources** console provides information about the sources of traffic on your FortiGate unit.

This console can be filtered by Country, Destination Interface, Policy, Result, Source, and Source Interface. For more on filters, see Filtering options.

Specific devices and time periods can be selected and drilled down for deep inspection.

Scenario: Investigating a spike in traffic

A system administrator notices a spike in traffic and wants to investigate it. From the **Sources** window, they can determine which user is responsible for the spike by following these steps:

1. Go to **FortiView > Sources**.
2. In the graph display, click and drag across the peak that represents the spike in traffic.
3. Sort the sources by bandwidth use by selecting the **Bytes (Sent/Received)** header.
4. Drill down into whichever source is associated with the highest amount of bandwidth use by double-clicking it. From this screen, you have an overview of that source's traffic activity.
5. Again, in either the **Applications** or **Destinations** view, select the **Bytes (Sent/Received)** header to sort by bandwidth use.
6. Double-click the top entry to drill down to the final inspection level, from which you can access further details on the application or destination, and/or apply a filter to prohibit or limit access.

Only FortiGate models 100D and above support the 24 hour historical data.

Destinations

The **Destinations** console provides information about the destination IP addresses of traffic on your FortiGate unit, as well as the application used. You can drill down the displayed information, and also select the device and time period, and apply search filters.

This console can be filtered by Country, Destination Interface, Destination IP, Policy, Result, and Source Interface. For more on filters, see Filtering options.

Scenario: Monitoring destination data

The Destinations console can be used to access detailed information on user destination-accessing through the use of the console's drilldown functionality. In this scenario, the console is used to find out more about a particular user's Facebook usage patterns over a 24-hour period:

1. Go to **FortiView > Destinations**.
2. Select **1 hour** from the Time Display options at the top right corner of the console.
3. The easiest way to locate most destinations is to scan the Applications column for the name of the application. Once the session containing Facebook has been located, double-click it to access the Destination summary window.
4. Locate Facebook in the Applications column and double-click it to view the Facebook drilldown page. From here, detailed information regarding the user's Facebook session can be accessed.

Only FortiGate models 100D and above support the 24 hour historical data.

Interfaces

The **Interfaces** console lists the total number of interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring, represented in both bytes sent and received, and the total bandwidth used.

This console can be filtered by Country, Destination Interface, Destination IP, Policy, Result, Source, and Source Interface. For more on filters, see Filtering options.

Only FortiGate models 100D and above support the 24 hour historical data.

Scenario: Investigate traffic spikes per user

The wan1 interface is showing a higher amount of traffic than usual. A system administrator uses the console to inspect which user (as represented by an IP address) is creating the spike in traffic:

1. Go to **FortiView > Interfaces** and double-click on wan1, or right click and select **Drill Down to Details...**.
2. The console will drill down to a summary page of wan1, showing how many bytes are being sent and received, how much bandwidth is being used, and how many sessions are currently using this interface. You see the IP address of the user that is showing the most amount of traffic under **Source**.
3. You can further drill down to see the IP destination, the device, and the applications being used, and other options.

Policies

The **Policies** console shows what policies are in affect on your network, what their source and destination interfaces are, how many sessions are in each policy, and what sort of traffic is occurring, represented in bytes sent and received.

This console can be filtered by Country, Destination Interface, Destination IP, Policy, Source, Source Device, and Source Interface. For more on filters, see Filtering options.

Only FortiGate models 100D and above support the 24 hour historical data.

Scenario: Investigate which policies are in effect

You can click on policy IDs to drill down to the policy list and see what policy's are in effect for specific interfaces, how many sessions have occurred, how many of those with the policy have been blocked, and more:

1. Go to **FortiView > Policies**, and double-click on a policy ID to drill down.
2. You will be redirected to a summary screen of the policy ID. From here you can view the source IP of where the policy has been used, what source interface has been using the particular policy, and to verify what sort of threat scores have been measured, both blocked and allowed.

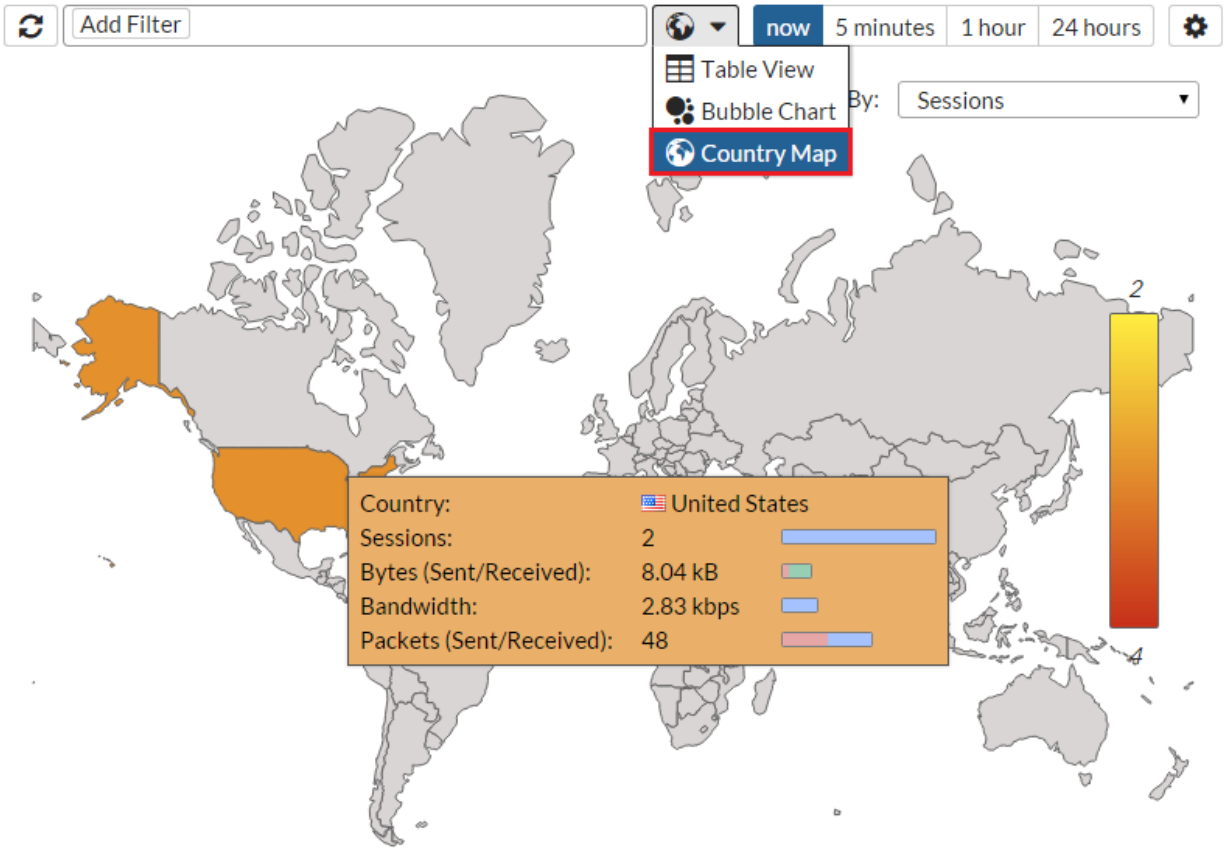
Countries

The **Countries**console displays network activity by geographic region. This console features the same view options as the other consoles, as well as Country Map. This visually highlights the countries from which user access to the network has been detected on a map of the globe.

The Time Display options for this console are 5 minutes, 1 hour, and 24 hours. The Country Map can sort by various options using the **Sort By:** dropdown menu. You can place your cursor over any country to display a tool-tip with detailed info on that country's traffic, and click on any country to drill down into greater (filtered) detail. The colour gradiant on the map indicates the traffic load, where red indicates the more critical load.

This console can be filtered by Country, Destination Interface, Policy, Result, and Security Interface. For more on filters, see Filtering options.

Only FortiGate models 100D and above support the 24 hour historical data.



Scenario: Investigate international source bandwidth usage

The Countries console can be used to investigate how much bandwidth specific international sources/IP addresses are using:

1. Go to **FortiView > Countries** to see what and how many countries are currently logged into the corporate network. You can also see how many sessions are taking place in each country, and how much traffic they are generating, shown by bytes sent and received, and total bandwidth usage.
2. To see how much specific bandwidth any particular session is using, drill down into a country, e.g. **United States**, and select the **Destinations** drill down option.
3. All current sessions from the United States are now shown in list format. From here you can select either **Bytes (Sent/Received)** and/or **Bandwidth** column headers to show which session is generating the most bandwidth, and exactly how much bandwidth is being used.

WiFi Clients

The **WiFi Clients** console shows a list of all the devices connected to the WLAN. The type of device, source, number of sources blocked and allowed, and bytes sent and received are displayed. The source's Service Set Identifier (SSID) is also displayed in the **Source SSID** column. An SSID is a case sensitive, 32 character alphanumerical identifier that acts as a password when a mobile device tries to connect to the WLAN.

This console can be filtered by AP, Device Type, Result, Source Device, Source IP, Source SSID, and User. For more on filters, see Filtering options.

Scenario: Determining the threat risk of an individual WiFi client

In this scenario,the administrator will use the WiFi Clients FortiView console to determine the risk levels associated with an individual WiFi client, and then drilldown into that client to determine where the risk originates and who might be the offending user/IP.

1. Go to **FortiView > WiFi Clients** and view the device list table.
2. Double-click on a device to filter on that source.
3. Under the **Risk** column, identify the items that present the greatest risk (using the **Applications**, **Destinations**, **Threats**, and/or **Sessions** tabs, for example).
4. Right-click these items for further action.

Traffic Shaping

The **Traffic Shaping** console provides information about FortiGate Traffic Shapers that are currently in effect. This console can be filtered by Traffic Shaper Name. For more on filters, see Filtering options.

A number of columns available in FortiView are only available in Traffic Shaping. For example, the **Shaper** column displays the name of the Shaper, which can be used to monitor the traffic being shaped by Bytes Sent, Received, and Dropped, so that bandwidth patterns and Shaper effectiveness can be analyzed.

Only FortiGate models 100D and above support the 24 hour historical data.

All Sessions

The **All Sessions** console provides information about all FortiGate traffic. This console can be filtered by Application, Country, Destination Interface, Destination IP, Destination Port, NAT Source IP, NAT Source Port, Policy, Protocol, Source, Source Interface, Source IP, and Source Port. For more on filters, see Filtering options.

This console has the greatest number of column options to choose from. To choose which columns you wish to view, select the column settings cog at the far right of the columns and select your desired columns. They can then be clicked and dragged in the order that you wish them to appear.

A number of columns available in FortiView are only available in All Sessions. For example, the **Action** column displays the type of response taken to a security event. This function can be used to review what sort of threats were detected, whether the connection was reset due to the detection of a possible threat, and so on. This would be useful to display alongside other columns such as the **Source**, **Destination**, and **Bytes (Sent/Received)** columns, as patterns or inconsistencies can be analyzed.

Similarly, there are a number of filters that are only available in All Sessions, one of which is **Protocol**. This allows you to display the protocol type associated with the selected session, e.g. TCP, FTP, HTTP, HTTPS, and so on.

Scenario: Filtering sessions by port number and application type

From the **All Sessions** console, a wide variety of filters can be applied to sort the session data. In this example, the All Sessions filters will be used to locate a specific user's recent Skype activity.

1. Go to **FortiView > All Sessions**.
2. Select **now** from the **Time Display** options if it is not already selected.
3. Select the **Filter** button, then select **Applications**. This will open a drop-down menu listing the applications that appear in the master session list. From this list, locate and select **Skype**, or type "Skype" into the Search Bar and hit **Enter**. This will filter the session list to only feature Skype usage.
4. Select the **Filter** button again, then select **Destination Port** from the drop-down menu, then locate and select the desired port number. This will add a second filter which will restrict the results to presenting only the Skype data associated with that port number.

Only FortiGate models 100D and above support the 24 hour historical data.

Applications

The **Applications** console provides information about the applications being used on your network.

This console can be filtered by Application, Country, Destination Interface, Policy, Result, and Source Interface. For more on filters, see Filtering options.

Specific devices and time periods can be selected and drilled down for deep inspection.

In order for information to appear in the **Applications** console, Application Control must be enabled in a policy.

Scenario: Viewing application usage

A manager is interested in the office internet habits of their employees:

1. Go to **FortiView > Applications**, to view the list of applications accessed by the users on your network. Use the time-frame options to view what applications were used in those time periods (from now, 5 minutes, 1 hour, or 24 hours).

2. From **Sessions (Blocked/Allowed)** and **Bytes (Sent/Received)**, you can see how much traffic has been generated. Click these columns to show the traffic in descending order.
3. You notice that a social media application has created the most traffic of all the applications, and so it's at the top of the list. Drill down into the application by double-clicking or right-clicking and select **Drill Down to Details**.
4. You are directed to a summary page of the social media application. From here, you can see which specific user has made the most use of the application.

Only FortiGate models 100D and above support the 24 hour historical data.

Cloud Applications

The **Cloud Applications** console provides information about the cloud applications being used on your network. This includes information such as:

- The names of videos viewed on YouTube (visible by hovering the cursor over the session entry)
- Filed uploaded and downloaded from cloud hosting services such as Dropbox
- Account names used for cloud services

Two different views are available for the Cloud Applications: **Applications** and **Users** (located in the top menu bar next to the time periods). **Applications** shows a list of the programs being used. **Users** shows information on the individual users of the cloud applications, including the username, if the FortiGate was able to view the login event.

This console can be filtered by Cloud Application and Result. For more on filters, see Filtering options.

In order for information to appear in the **Cloud Applications** console, an application control profile (that has Deep Inspection of Cloud Applications turned on) must be enabled in a policy, and SSL Inspection must use `deep-inspection`.

Scenario: Viewing cloud application usage data

From the Cloud Applications console, users can drill down to access detailed data on cloud application usage data. In this scenario, the console is used to determine the network's most frequent user of YouTube over a 24-hour period, and find out more about their usage patterns.

1. Go to **FortiView > Cloud Applications**.
2. Select **Applications** view from the top menu bar if it is not already selected.
3. Select **24 Hours** from the Time Display options.
4. Find **YouTube** under the Application column and double-click it (or right-click and select **Drill down for details...**). This will open the YouTube stats window.
5. To determine the user who has accessed YouTube the most frequently, sort the column entries by **Sessions** by selecting the column header of the same name.
6. Double-click (or right-click and select **Drill down for details...**) the top-bandwidth YouTube user to view detailed stats, including the names of videos watched by the user and the date and time each video was accessed.

Only FortiGate models 100D and above support the 24 hour historical data.

Web Sites

The **Web Sites** console lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be selected in order to see a description of the category and several example sites, with content loaded from FortiGuard on demand.

This console can be filtered by Domain and Result. For more on filters, see Filtering options.

In order for information to appear in the **Web Sites** console, web filtering must be enabled in a policy, with FortiGate Categories enabled.

Scenario: Investigating an instance of Proxy Avoidance

In this scenario, the Categories view will be used to investigate an instance of Proxy Avoidance, one of the Categories recognized by FortiOS. Proxy Avoidance denotes the use of a proxy site in order to access data that might otherwise be blocked by the server.

1. Go to **FortiView > Web Sites** to open the Web Sites console.
2. Select **Categories** from the top bar menu to enter Categories view.
3. Scan the **Categories** column and locate the instance of Proxy Avoidance, then double-click it to enter its drilldown screen.

Only FortiGate models 100D and above support the 24 hour historical data.

Threats

The **Threats** console lists the top users involved in incidents, as well as information on the top threats to your network.

The following incidents are considered threats:

- Risk applications detected by application control
- Intrusion incidents detected by IPS
- Malicious web sites detected by web filtering
- Malware/botnets detected by antivirus

This console can be filtered by Country, Destination Interface, Policy, Result, Security Action, Source Interface, Threat, and Threat Type. For more on filters, see Filtering options.

In order for information to appear in the **Threats** console, Threat Weight Tracking must be enabled.

Scenario: Monitoring Threats to the Network

Some users have high Threat Scores. The Threats console can be used to view all threats and discover why such high scores are being shown:

1. Go to **FortiView > Threats**. In the graph display, click and drag across the peak that represents the spike in threat score.
2. Sort the threats by score or level by selecting the **Threat Score (Blocked/Allowed** or the **Threat Level** headers respectively.
3. You see that a specific threat's Threat Level is at Critical. Drill down into the threat by double-clicking or right-clicking and select **Drill down to details**.
4. From this summary page, you can view the source IPs and the number of sessions that came from this threat. Double-click on one of them.
5. The following page shows a variety of statistics, including **Reference**. The URL next to it will link you to a FortiGuard page where it will display the description, affected products, and recommended actions, if you are not familiar with the particular threat.

Only FortiGate models 100D and above support the 24 hour historical data.

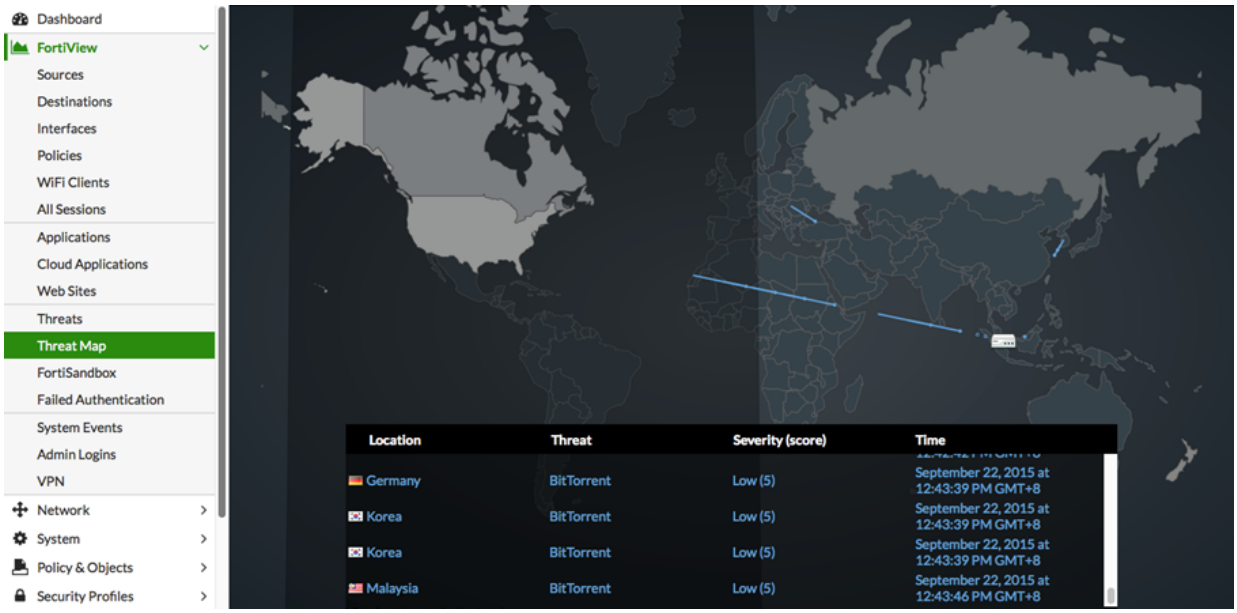
Threat Map

The **Threat Map** console displays network activity by geographic region. Threats from various international destinations will be shown, but only those arriving at your destination, as depicted by the FortiGate. You can place your cursor over the FortiGate's location to display the device name, IP address, and the city name/location.

A visual lists of threats is shown at the bottom, displaying the location, severity, and nature of the attacks. The color gradient of the darts on the map indicate the traffic risk, where red indicates the more critical risk.

Unlike other FortiView consoles, this console has no filtering options, however you can click on any country to drill down into greater (filtered) detail.

Only FortiGate models 100D and above support the 24 hour historical data.



Scenario: Investigate various international threats

The Threat Map console can be used to regionalize areas that you are more interested in, and disregard regions that you are not interested in:

1. Go to **FortiView > Threat Map** to see a real-time map of the globe. This will show various incoming threats from multiple destinations around the world, depending upon where the FortiGate is placed on the map.
2. You are not interested with threats that are being sent to Eastern Europe, however you are concerned with threats that may be sent to a city in North America. Click and drag the FortiGate to the approximate location where you would like to monitor the incoming threats.
3. To see which countries are sending the more severe threats to your region/location, either see where the red darts are coming from, or check the visual lists of threats at the bottom.

FortiSandbox

The **FortiSandbox** console detects and analyzes advanced attacks designed to bypass traditional security defenses, and has a wide array of features that allow it to prevent future attacks from occurring again.

This console can be filtered by Checksum, File Name, Source, Status, and User Name. For more on filters, see Filtering options.

Only FortiGate models 100D and above support the 24 hour historical data.

Failed Authentication

The **Failed Authentication** console displays instances in which users attempted to connect to the server but were unsuccessful. Depending on the Time Display setting, the console will display instances from the last 5 minutes, 1 hour, or 24 hours. The results can be sorted by the number of instances a given user attempted to log in.

By double-clicking on any of the entries on the main Failed Authentication console, a drill down view appears, displaying more detailed information on that user's authentication attempts, including the date and time of each login attempt, the message explaining the reason each authentication failed e.g. a mismatched password, and the source IP address.

This console can be filtered by Destination, Login Type, Result, Source, Type, and User. For more on filters, see Filtering options.

Only FortiGate models 100D and above support the 24 hour historical data.

Scenario: Investigating a user's failed authentication attempts

The Failed Authentications console can be used to access information on individual users and their unsuccessful attempts to access the network. In this scenario, an administrator investigates a user's multiple attempts via the console's drill down capability.

1. Go to **FortiView > Failed Authentication** to access the Failed Authentication console.
2. Select the **Failed Attempts** column header to sort the entries by number of attempts.
3. Double-click the top entry to drill down to more detailed information on attempts made by the user with the highest number of attempts.

System Events

The **System Events** console lists security events detected by FortiOS, providing a name and description for the events, an assessment of the event's severity level (**Alert**, **Critical**, **Emergency**, **Error**, or **Warning**), and the number of instances the events were detected.

This console can be filtered by Event Name, Result, and Severity. For more on filters, see Filtering options on page 44.

Scenario: Investigate network security events

System Events can be used in conjunction with All Sessions to see what network security events took place, and specifically see what action was taken upon their detection:

1. Go to **FortiView > System Events** to see what and how many network events have taken place, as well as how severe they are in terms of the threat they pose to the network.
2. You see that a particular event has warranted a severe rating, and has allowed traffic to bypass the firewall. Note when the event took place, and go to **FortiView > All Sessions**, to see more information pertaining to the security event.

3. From this console, you can determine the system event's source, how much traffic was sent and received, and the security action taken in response to this security event. These actions differ, depending upon the severity of the security event. See the entry for **Security Action** in Columns displayed on page 48.

Only FortiGate models 100D and above support the 24 hour historical data.

Admin Logins

The **Admin Logins** console provides information on administrator interactions with the network, including the number of login instances, number of failed logins, and the length of time logged in. This console features the same view options as the other consoles, as well as Timeline View.

This console can be filtered by Result and User Name. For more on filters, see Filtering options.

Scenario: Scrutinizing Administrator Security

Admin Logins can be used in conjunction with **System Events** to see who was on during a system change that impacted performance and allowed a threat to persist/pass through the firewall:

1. Go to **FortiView > System Events**, to see what and how many network events have taken place, as well as how severe they are in terms of the threat they pose to the network.
2. You see that a particular event has warranted a severe rating, and has allowed traffic to bypass the firewall. Double-click on the event to drill down.
3. Once drilled down, you can see the date and time that the system change took place.
4. Go to **FortiView > Admin Logins**, to see who has been logged in, how long they have been logged in, and what configuration changes they have made. Using the time graph, you can correlate the information from System Events with who was logged in at the time the threat was allowed.

Only FortiGate models 100D and above support the 24 hour historical data.

VPN

From the **VPN** console, users can access information on any VPNs associated with their FortiGate. From the initial window, a list of all the associated VPNs is provided, along with general information, such as number of user connections and VPN type. By double-clicking on an individual VPN (or right-clicking and selecting **Drill down for details...**), users can access more specific data on that VPN.

Logs in the VPN console can be sorted by number of connections, last connection time, or data sent/received by selecting the column headers.

This console can be filtered by Result, User Name, and VPN Type. For more on filters, see Filtering options on page 44.

Certain dashboard options will not appear unless your FortiGate has Disk Logging enabled.

Furthermore, only certain FortiGate models support Disk Logging — refer to the FortiView Feature Support - Platform Matrix on page 18 for more information.

To enable Disk Logging, go to **Log & Report > Log Settings**, and select the checkbox next to **Disk** and apply the change.

Scenario: Investigating VPN user activity

The VPN console can be used to access detailed data on VPN-user activity via the use of the drill down windows. In this scenario, the administrator looks into the usage patterns of the IPsec user who has most frequently connected to the network.

1. Go to **FortiView > VPN** to view the VPN console.
2. Select the **Connections** column header to sort the entries by number of connections to the network.
3. Locate the top user whose VPN Type is **ipsec** and double-click the entry to enter that user's drill down screen.
4. To get the most representative data possible, sort the entries by bandwidth use by selecting the **Bytes (Sent/Received)** column header. Double-click the top entry to enter the drill down window for that connection instance.
   From this screen, the administrator can find out more about the specific session, including the date/time of access, the XAuth (Extensible Authentication) User ID, the session's Tunnel ID, and more.

Only FortiGate models 100D and above support the 24 hour historical data.

Reference

This section consists of reference information for the various consoles in FortiView. Each console has an assortment of filtering options, drilldown options, and columns that can be displayed. Since many of these options and columns persist through each console, the entire list of options and their descriptions is included below. Attempts have been made to identify the instances where an option or column is only available to a particular console.

This section includes:

Filtering options

When you select the **Add Filter** button, a drop-down list appears with a list of available filtering options. Available options differ based on which console is currently being viewed. The following table explains all of the available filtering options:

Filter option	Description
Accelerated Sessions	You can filter the console on 'FortiASIC' ('Accelerated' versus 'Not Accelerated') sessions.
AP	Filter by Access Point (AP) identification number.
Application	Filter by application name.
Checksum	Filter by checksum value. Checksums are reference digits used to represent the correct datasum of a packet in order to detect errors.
Cloud Application	Filter by cloud application name. **Note:** This filter is only available in the **Cloud Applications** console.
Country	Filter by the country from which the source accessed the server.
Destination Interface	Filter by the interface type used by the destination user, e.g. wan1.
Destination IP	Filter by the IP address used by the destination.

Filter option	Description
Destination Port	Filter by the port used by the destination. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Domain	Filter by domain name. **Note:** This filter is only available in the **Web Sites** console.
Event Name	Filter by security event name. **Note:** This filter is only available in the **System Events** console.
File Name	Filter by file name. **Note:** This filter is only available in the **FortiSandbox** console.
Login Type	Filter by type of login (eg. WEP) associated with the displayed authentication attempt. **Note:** This filter is only available in the **Failed Authentications** console.
NAT Source IP	Filter by the NAT-translated source IP address. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
NAT Source Port	Filter by the NAT-translated source interface. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Policy	Filter by the policy identification number.
Protocol	Filter by the protocol used by the source, e.g. tcp or udp. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Result	Filter by the result of whatever security action was taken by FortiOs in the selected session, eg. Accept (all).

Filter option	Description
Security Action	Filter by the type of response taken to the security event. The types of possible actions are as follows: **Allowed:** No threat was detected and the connection was let through. **Blocked:** A threat was detected and the connection was not let through. **Reset:** A possible issue was detected and the connection was reset. **Traffic Shape:** Some data packets may have been delayed to improve system-wide performance.
Severity	Filter by the severity level (**Critical**, **High**, **Medium** or **Low**) associated with a security event.
Source **Source IP**	Filter by the source IP address.
Source Device	Filter by source device type, e.g. mobile.
Source Interface	Filer by the interface type used by the source user, e.g. wan1.
Source Port	Filter by the source interface. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Source SSID	Filter by the Service Set Identifier (SSID) associated with the selected user. An SSID is a case sensitive, 32 character alphanumerical identifier that acts as a password attributed to a mobile device.
Status	Filter by the maliciousness of a file. The types of possible status' are **Malicious**, **High**, **Medium**, **Low**, **Clean**, **Unknown**, and **Pending**. **Note:** This filter is only available in the **FortiSandbox** console.
Threat	Filter by threat name and/or URL
Threat Type	Filter by threat category, e.g. *Illegal/Unethical* or *P2P*.
Type	**Note:** This filter is only available in the **Failed Authentications** console.
User Name	Filter by user name.
VPN Type	Filter by Virtual Private Network (VPN) protocol type, eg. *PPTP*. **Note:** This filter is only available in the **VPN** console.

Drill down options

Double-click, or right-click, on any entry in a FortiView console and select **Drill Down to Details**, to view the following columns (options vary depending on the console selected):

Drill down options are available for all FortiView consoles except **All Sessions**, **Logical Topology**, and **Physical Topology**.

Option	Description
Applications	Select to drill down by application to view application-related information, including the application name, sessions blocked and allowed, bytes sent and received, and the risk level. You can sort entries by selecting the column header.
Sources	Select to drill down by rows to view source-related information, including IP address, device type, interface type, threat score, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.
Destinations	Select to drill down by destination to view destination-related information, including the IP address and geographic region, interface, threat score, number of sessions blocked and allowed, and bytes sent and received. You can sort entries by selecting the column header.
Countries	Select to drill down by country, including the number of sessions, bytes sent and received, and the bandwidth used.You can sort entries by selecting the column header.
Policies	Select to drill down by the policies in use, including source interface, destination interface, bytes sent and received, and bandwidth used. You can sort entries by selecting the column header.
Source Interfaces	Select to drill down by source interface, including bytes sent and received, and bandwidth used. You can sort entries by selecting the column header.
Destination Interfaces	Select to drill down by destination interface, including bytes sent and received, and bandwidth used. You can sort entries by selecting the column header.
Threats	Select to drill down by threat to view threat-related information, including the threat name, category, threat level, threat score, and number of sessions blocked and allowed. You can sort entries by selecting the column header.
Domains	Select to drill down by domain to view domain-related information, including domain name, category, browsing time, threat weight, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.
Categories	Select to drill down by category to view category-related information, including category name, browsing time, threat score, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.

Option	Description
Sessions	Select to drill down by sessions to view session-related information, including date/time, source, destination IP address and geographic region, application name,security action, security event, and bytes sent/received. You can sort entries by selecting the column header.

Columns displayed

The following columns appear in the initial window of the dashboards. Some columns may only be visible by selecting them from the column drop-down menu. Options vary depending on the dashboard selected.

Column name	Description
Action	Displays the type of response taken to a security event. The types of possible actions are as follows: • **Allowed**: No threat was detected and the connection was let through. • **Blocked**: A threat was detected and the connection was not let through. • **Reset**: A possible issue was detected and the connection was reset. • **Traffic Shape**: Some data packets may have been delayed to improve system-wide performance. **Note:** This column is only available in the **All Sessions** console.
Application	Displays the application name and service. When **Time Display** is set to **now**, you can access further information about an application by selecting the column entry.
Application Category	Displays the type of application used in the selected session, e.g. video player, social media. **Note:** This column is only available in the **All Sessions** console.
Application ID	Displays the identification number associated with the application used in the selected session. **Note:**This column is only available in the **All Sessions** console.

Column name	Description
Application Risk **Risk**	Displays the application risk level. You can hover the mouse cursor over the entry in the column for additional information, and select the column header to sort entries by level of risk. Risk uses a 5-point risk rating. The rating system is as follows: • **Critical**: Applications that are used to conceal activity to evade detection. • **High**: Applications that can cause data leakage, are prone to vulnerabilities, or may download malware. • **Medium**: Applications that can be misused. • **Elevated**: Applications that are used for personal communications or can lower productivity. • **Low**: Business-related applications or other harmless applications.
Bandwidth	Displays information for bandwidth calculated on a per-session level, providing administrators the ability to sort realtime bandwidth usage in descending order.
Browsing Time	Displays the amount of time a user has spent browsing a web site (in seconds). **Note:** This column is only available in the **Web Sites** console, in **Categories** view..
Bytes (Sent/Received)	Displays the size of sent and received data packets, as measured in bytes. Select the column header to sort the entries by size. **Note:** This information is available on some consoles as two separate columns: **Sent** and **Received**.
Category	Displays the category descriptor appropriate to whatever console is being displayed. For example, threat categories are displayed in the Threats console.
Cloud User	Displays the users accessing cloud applications by IP address. **Note:** This column is only available in the **Cloud Applications** console, in **Users** view.
Configuration Changes	Displays the number of configuration changes made by the user. You can hover the mouse cursor over an entry for additional information. **Note:** This column is only available in the **Admin Logins** console.

Column name	Description
Connections	Displays the number of VPN connections made by the selected user.. **Note:** This column is only available in the **VPN** console.
Country	Displays the country from which the selected traffic is originating. **Note:** This column is only available in the **Countries** console.
Destination	Displays the destination name, IP address and geographic region.
Destination Country	Displays the country session data is being sent to. **Note:** This column is only available in the **All Sessions** console.
Destination Interface	Displays which interface session data is being sent through, e.g. wan1.
Destination Port	Displays the port number of the destination server being used to accept data. Note: This column is only available in the **All Sessions** console.
Device	Displays the device IP address or Fully Qualified Domain Name (FQDN).
Domain	Displays the domain associated with the selected web site, e.g. google.com. **Note:** This column is only available in the **Web Sites** console.
DST Nat IP **NAT Destination**	Displays the Network Address Translation (NAT) IP address associated with the destination server. **Note:** This column is only available in the **All Sessions** console.
DST Nat Port **NAT Destination Port**	Displays the Network Address Translation (NAT) port number associated with the destination server. **Note:** This column is only available in the **All Sessions** console.
Duration	Displays the amount of time (in seconds) a user has been logged in. **Note:** This column is only available in the **Admin Logins** console.
Event Name (Description)	Displays the name and description of the selected security event. **Note:** This column is only available in the **System Events** console.

Column name	Description
Events	Displays the number of security events that occurred within a selected session. **Note**: This column is only available in the **System Events** console.
Expires	Displays the amount of time a session has (in seconds) before it is set to expire. **Note:** This column is only available in the **All Sessions** console, in **now** Time Display view.
Failed Logins	Displays the number of failed login attempts made by an administrator over the specified time period. **Note:** This column is only available in the **Admin Logins** console.
Files (Up/Down)	Displays the number of files uploaded and downloaded. Hover the mouse cursor over the entry in the column for additional information. **Note:** This column is only available in the **Cloud Applications** console.
FortiASIC	Displays the type of FortiASIC hardware acceleration used in the specified session, if present. **Note:** This column is only available in the **All Sessions** console, in the **now** Time Display view.
Group	Displays the group ID associated with the selected session. **Note:** This column is only available in the **All Sessions** console.
Last Connection Time	Displays the most recent instance of connection to the selected Virtual Private Network (VPN). **Note:** This column is only available in the **VPN** console.
Level **Threat Level**	Displays the threat level. Select the column header to sort entries by threat level.
Log ID	Displays the identification number for the data log associated with this entry. **Note:** This column is only available in the **All Sessions** console.

Column name	Description
Login IDs	Displays the number of login IDs associated with the selected cloud application. **Note:** This column is only available in the **Cloud Applications** console, in **Applications** view.
Login Type	Displays the type of login (eg. WEP) associated with the displayed authentication attempt. **Note:** This column is only available in the **Failed Authentications** console.
Logins	Displays the number of successful logins made by an administrator over the specified time period. **Note:** This column is only available in the **Admin Logins** console.
Pending	**Note:** This column is only available in the **FortiSandbox** column, in **Source** view.
Policy ID	Displays the identification number of the policy under which the selected connection was allowed.
Security Action	Displays the action taken in response to the selected security event. The types of possible actions are as follows: • **Allowed**: No threat was detected and the connection was let through. • **Blocked**: A threat was detected and the connection was not let through. • **Reset**: A possible issue was detected and the connection was reset. • **Traffic Shape**: Some data packets may have been delayed to improve system-wide performance.
Sessions	Displays the number of sessions associated with the selected destination. **Note:** This column only appears in the **Destinations** console, in the **now** Time Display view.
Sessions (Blocked/Allowed)	Displays the number of sessions blocked and allowed by FortiOs. In some consoles, entries can be sorted by number of sessions by selecting the column header..
Severity	Displays the severity level (**Critical**, **High**, **Medium** or **Low**) associated with the selected security event.

Column name	Description
Source	Displays the source IP address and/or user ID, if applicable.
Source Interface	Displays which interface is being used by the destination server (eg. wan1).
Source Port	Displays the port number being used by the source server to send data.
Source SSID	Displays the Service Set Identifier (SSID) associated with the selected user. **Note:** This column is only available in the **Wifi Clients** console.
Src NAT IP **NAT Source**	Displays the Network Address Translation (NAT) IP address associated with the source server.
Src NAT Port **NAT Source Port**	Displays the Network Address Translation (NAT) port number associated with the source server.
Status	The types of possible status' are **Malicious**, **High**, **Medium**, **Low**, **Clean**, **Unknown**, and **Pending**. **Note:** This console is only available in the **FortiSandbox** console, in **Files** view.
Submitted	Displays the number of files submitted to the FortiSandbox for assessment in the selected session. **Note:** This column is only available in the **FortiSandbox** console, in **Files** view.
Threat	Displays the threat type detected in the selected session.
Threat Score (Blocked/Allowed)	Displays the threat score value, a measurement of the total number of threats detected over the course of the session. You can select the column header to sort entries by threat score.
Threat Weight	Displays the threat weight profile associated with the selected session.
Timestamp	Displays the selected session's PHP timestamp.
User **User Name**	Displays the user name associated with the selected administrator.

Column name	Description
Videos Played	Displays the number of videos played via cloud applications. **Note:** This column is only available in the **Cloud Applications** console.

Risk level indicators

There are currently two consoles within FortiView that display the Risk associated with the console: **Applications** and **Cloud Applications**. Each application pose different levels of risk to the network, represented by a colour code.

The following table identifies each risk level, from least to most severe:

Indicator	Risk	Description
	**Green:** *Risk Level 1*	These applications have little to no risk level, with no assigned risk definition. Application file-sharing may result in data leakage, which would be a typical example of a low level risk. An example application would be the Google toolbar, or Dropbox.
	**Blue:** *Risk Level 2*	These applications have an elevated risk level and typically use excessive bandwidth. High bandwidth consumption can lead to increased operational costs. An example application would be Bittorrent.
	**Yellow:** *Risk Level 3*	These applications have a low risk level and are typically evasive. Evasive applications can lead to compliance risks, and could include applications such as JustinTV and GlypeProxy.
	**Orange:** *Risk Level 4*	These applications have a high risk level, and are defined as using both excessive and evasive bandwidth. Example applications would be AutoHideIP and PandoraTV.
	**Red:** *Risk Level 5*	Applications that have a high risk level are prone to malware or vulnerabilities that can introduce business continuity risks.

Troubleshooting FortiView

No logging data is displayed

In order for information to appear in the FortiView consoles, disk logging must be selected for the FortiGate unit. To select disk logging, go to **Log & Report > Log Settings**.

Disk logging is disabled by default for some FortiGate units. To enable disk logging, enter the following command in the CLI:

```
config log disk setting
   set status enable
end
```

Only certain FortiGate models support Disk Logging — refer to the FortiView Feature Support - Platform Matrix on page 18 for more information.

Logging is enabled, but data is not appearing

Some FortiView consoles require certain features to be enabled and working before they will display any data. For example, the Web Filtering FortiView page requires that a Web Filtering profile be configured in **Security Profiles > Web Filter** and then applied to a policy in **Policy & Objects > IPv4 Policy**.

First, ensure the feature is enabled in **System > Feature Select**, and then go to the appropriate page to make sure that the feature is being implemented. If it is working but is producing no data, FortiView will have nothing to display.

FORTINET®

High Performance Network Security